Lower bounds for some decision problems over $\mathbb{C}$

Gregorio Malajovich*

January 22, 1999

Abstract

Lower bounds for some explicit decision problems over the complex numbers are given.

1 Introduction

This paper is about lower bounds for certain decision problems over $\mathbb{C}$. (See [3] for the model of computation and for background). In particular, we will provide lower bounds for the complexity of deciding, given x, if $p^d(x) = 0$ for some explicit polynomials p^d.

A related problem is to give lower bounds for the evaluation of explicit polynomials. This has been an active subject of research since [6]. See [4] for modern developments and for bibliographical remarks. More recent results appeared in [1] and [2].

Most of those bounds use the Ostrowsky model of computation ([4] page 6): sum and multiplication by an algebraic constant are free, and the complexity of a computation for polynomial $f(x)$ is the number of non-scalar multiplications, i.e., of multiplications of two polynomials in the variable x. For instance, Horner rule for a degree d polynomial requires d non-scalar multiplications.

All those bounds apply trivially to the complexity of evaluating polynomials by a 'machine over $\mathbb{C}$' as defined in [3], or to the (multiplicative-branching) complexity of a computation tree for evaluating the same polynomial.

Little is known, however, about the application of those bounds to decision problems (Over $\mathbb{C}$, in the sense of [3], or by a decision tree as in [4], Definition (4.19) page 115. In this definition, each node of a computation tree can perform one algebraic operation or comparison, and therefore a natural measure of complexity is the depth of the tree).

In this paper, only decision problems of the form below will be considered: let $X \subseteq \mathbb{N} \times \mathbb{C}$, and let $X_d = \{x \in \mathbb{C} : (d, x) \in X\}$. Typically, d is the problem size and $\#X_d \leq d$. One can think of X as the disjoint union of the zero-set of a

*Departamento de Matemática Aplicada, Universidade Federal do Rio de Janeiro. Caixa Postal 68530, CEP 21945, Rio de Janeiro, RJ, Brasil. e-mail: gregorio@labma.ufrj.br. On leave at MSRI, 1000 Centennial Drive, Berkeley CA 94720-5070. e-mail: gregorio@msri.org

family of polynomials of degree $\leq d$, where $d \in \mathbb{N}$. The two following forms of a decision problem are natural in this setting:

Problem 1. For any fixed d, decide wether $x \in X_d$.

Problem 2. Decide wether $(d, x) \in X$

Problem 1 is non-uniform, in the sense that we allow for a different machine over $\mathbb{C}$ or a different decision tree to be used for each value of d. However, we want a bound on the running time or on the multiplicative complexity of the tree, as a function of d.

Problem 2 is uniform. It is harder than Problem 1, in the sense that it cannot be solved by a decision tree, since $\#X_d$ can be arbitrarily large. It requires a machine over $\mathbb{C}$, that will eventually branch according to the value of d.

Lower bounds for Problem 1 are also lower bounds for Problem 2.

A trivial, topological lower bound for Problems 1 and 2 when $\#X_d = d$ is $\log_2 d$. Sharper known bounds come from the 'Canonical Path' argument, see [3] section 2.5: Let f be a univariate polynomial. The complexity of deciding $f(x) = 0$ is bounded below by the minimum of the complexity of evaluating $g(x)$, where g ranges over the non-zero multiples of f.

If one assumes some property of f that propagates to its multiple g, then one eventually obtains a sharper, non-trivial lower bounds.

In Lemma 1 below, we will give conditions on the roots of f that will provide lower bounds for the evaluation of g. Essentially, we will require a subset of the roots to be rapidly growing. This will imply a rapid growth property for the coefficients of g. Then, the results of [1, 2] imply a lower bound for the complexity of evaluating g. Thus we will be able to construct specific polynomials that are hard to decide in the *non-uniform* sense, viz.

Lower bound 1. *The set $X = \{(d, x) \in \mathbb{Z} \times \mathbb{C} : x = 2^{2^{di}}, 0 \leq i \leq d$, cannot be solved in time polylog(d) in the setting of Problem 1.*

Lower bound 2. *The set $Y = \{(d, x) \in \mathbb{Z} \times \mathbb{C} : p^d(x) = 0\}$, where $p^d(t) = \sum_{i=0}^{d} 2^{2^{d(d-i)}} t^i$, cannot be decided in time polylog(d) in the setting of Problem 1.*

In a more classical computer-science language, we can define the input size of some (d, x) as $\log d$. This means that the integer d is represented in binary notation, while variable x can contain an arbitrary complex number. In that case, 'time polylog(d) in the setting of Problem 1' can be refrased as $\mathcal{P}_{/\text{poly}}$. The lower bounds above become now: $X \notin \mathcal{P}_{/\text{poly}}$ and $Y \notin \mathcal{P}_{/\text{poly}}$.

Non-uniform lower bounds 1 and 2 can be compared to the following easier, uniform lower bound:

Lower bound 3. *The set $Z = \{(d, x) \in \mathbb{Z} \times \mathbb{C} : q^d(x) = 0\}$, where $q^d(t) = \sum_{i=0}^{d} 2^{2^i} t^i$, cannot be decided in time polylog(d) in the setting of Problem 2.*

This means that the set Z, where d is represented in binary notation and x is a complex number, does not belong to $\mathcal{P}$ over $\mathbb{C}$.

This work was written while the author was visiting the Mathematical Sciences Research Institute, Berkeley, CA. Thanks to Pascal Koiran, José Luis Montaña, Luis Pardo and Steve Smale for their suggestions and comments.

2 Background and notations

Definition 1. Let $K \subset L$ be finite algebraic extensions of $\mathbb{Q}$. Let ν be a valuation in M_K. Then we extend the notation ν to L by:

$$\nu(x) = \frac{\sum_\mu n_\mu \mu(x)}{\deg[L:K]}$$

where the sum ranges over all the valuations μ of L that are 'above' ν, and where n_μ is the 'local degree' of $L : K$. The local degree is defined as $n_\mu = \deg[L_\mu : K_\nu]$, where K_ν is the completion of K under the metric induced by the absolute value $|.|_\nu$.

Recall that for $x \in K$, $\deg[L : K]\nu(x) = \sum_\mu n_\mu \nu(x)$. The case $K = \mathbb{Q}$ is an immediate consequence of Corollary 2 of Theorem 1 in Chapter II, p. 39 of [5].

Definition 2. Let g be a polynomial with algebraic coefficients in some extension K of $\mathbb{Q}$. Let ν be a valuation in M_K. The *Newton diagram* of g at ν is the (lower) convex hull of the set $\{(i, \nu(g_i)), i = 0 \cdots d\}$.

The basic property of Newton diagrams used here is the following.

Proposition 1. *Suppose that $\zeta_1, \cdots, \zeta_d$ are the roots of a univariate polynomial $g \in K[x]$. Let the roots of g be ordered so that*

$$\nu(\zeta_1) \geq \cdots \geq \nu(\zeta_d)$$

and let the increasing sequence i_j assume the values 0, d and all the values of i where:

$$\nu(\zeta_i) > \nu(\zeta_{i+1})$$

Then the sharp corners of the Newton diagram are precisely the points of the form $(i_j, \nu(g_{i_j}))$ for all j.

Moreover, the slope of the segment $[(i_{j-1}, \nu(g_{i_{j-1}})), (i_j, \nu(g_{i_j}))]$ is precisely $-\nu(\zeta_{i_j})$.

Proof of Proposition 1. The proof uses the following property of valuations: $\nu(\sum x_i) \geq \min \nu(x_i)$. Furthermore, when that minimum is attained in only one x_i, we have equality.

Let $i_{j-1} < k < i_j$. Writing

$$\begin{aligned} g_{i_{j-1}} &= g_d \sigma_{d-i_{j-1}}(\zeta_1, \cdots, \zeta_d) \\ g_k &= g_d \sigma_{d-k}(\zeta_1, \cdots, \zeta_d) \\ g_{i_j} &= g_d \sigma_{d-i_j}(\zeta_1, \cdots, \zeta_d) \end{aligned}$$

one can pass to the valuation by:

$$\begin{aligned} \nu(g_{i_{j-1}}) &= \nu(g_d) + \nu(\zeta_{i_{j-1}+1}) + \cdots + \nu(\zeta_d) \\ \nu(g_k) &\geq \nu(g_d) + \nu(\zeta_{k+1}) + \cdots + \nu(\zeta_d) \\ \nu(g_{i_j}) &= \nu(g_d) + \nu(\zeta_{i_j+1}) + \cdots + \nu(\zeta_d) \end{aligned}$$

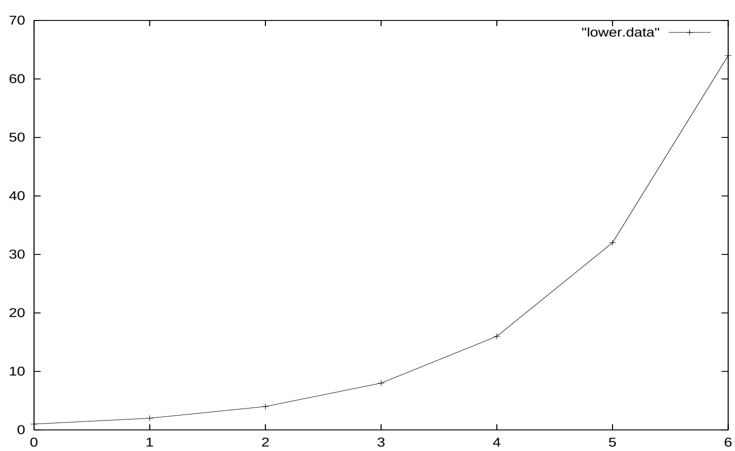
Subtracting, one obtains:

$$\begin{aligned} \nu(g_{i_j}) - \nu(g_{i_{j-1}}) &= -\nu(\zeta_{i_{j-1}+1}) - \cdots - \nu(\zeta_{i_j}) \\ &= -(i_j - i_{j-1})\nu(\zeta_{i_j}) \\ \nu(g_{i_j}) - \nu(g_k) &\leq -\nu(\zeta_{k+1}) - \cdots - \nu(\zeta_{i_j}) \\ &\leq -(i_j - k)\nu(\zeta_{i_j}) \end{aligned}$$

This concludes the proof. $\square$

3 Uniform lower bounds

We can now prove Lower Bound 3.



Proof of Lower bound 3. The Newton diagram of q^d at 2 is $\{(i, 2^i) : 0 \leq i \leq d\}$. (This latest set is convex, since the points lie on the curve $y = 2^x$ and this curve is convex). Therefore, there is a unique root ζ of q^d that minimizes $\nu(\zeta)$.

Since $q^d_{d-1} = (-\sum \zeta_i) q^d_d$, where the sum ranges over all the roots, we have:

$$\nu_2(q^d_{d-1}) = \nu_2(q^d_d) + \min \nu_2(\zeta_i) = \nu_2(q^d_d) + \nu_2(\zeta)$$

Replacing by the actual values of the coefficients, one gets:

$$\nu_2(\zeta) = -2^{d-1} \tag{1}$$

Now, suppose that there is a machine M that decides $q^d(t) = 0$ in time polylog(d). One can assume without loss of generality that this machine has no constant but 0 and 1. Let its running time be bounded by $T = a(\log d)^b$.

Let us fix $d > 2 + T^2$. We will derive a contradiction.

Let g be the polynomial defining the canonical path (recall that d is fixed now, so this is the path followed by generic $t \in \mathbb{C}$). It can be computed in time $\leq T^2$, so we have the following bounds:

$$\begin{aligned} \deg g &\leq 2^{T^2} \\ 0 \leq \nu_2(g_p) &\leq 2^{T^2} \end{aligned}$$

Since ζ is also a root of g, there are coefficients g_i and g_j, $i \neq j$, such that:

$$(j - i)\nu_2(\zeta) = \nu_2(g_i) - \nu_2(g_j) \tag{2}$$

Thus, $|\nu_2(\zeta)| \leq |\nu_2(g_i)| + |\nu_2(g_i)|$. This implies:

$$|\nu_2(\zeta)| \leq 2^{1+T^2} < 2^{d-1}$$

Replacing by equation 1, one obtains $2^{d-1} < 2^{d-1}$, a contradiction. $\square$

4 Non-uniform lower bounds

Lemma 1. *Let $g = g(t)$ be a degree D polynomial with algebraic coefficients. Let ν be a (non-archimedian) valuation of $K = \mathbb{Q}[g_0, \cdots, g_D]$. Let $\xi_1, \cdots \xi_D$ be the roots of g, and assume they are ordered in such way that:*

$$\nu(\xi_1) \geq \cdots \geq \nu(\xi_D)$$

Suppose that there is a subsequence $\zeta_j = \xi_{i_j+1}$, $j = 1 \cdots d$, such that the following holds:

1. $\nu(\zeta_d) \geq 1$
2. $\nu(\zeta_j) \geq 2(i_{j+1} - i_j)\ \nu(\zeta_{j+1})$, *for* $0 \leq j \leq d-1$.

Then g cannot be evaluated in less than

$$L \geq \sqrt{\frac{d}{28\log_2 D+1}}$$

multiplications.

Proof of Lemma 1. We can assume without loss of generality that the ordering of the ξ_i satisfies:

$$\cdots \xi_{i_j} < \xi_{i_j+1} = \zeta_j \leq \xi_{i_j+2} \cdots$$

For $j \in \{1, \cdots, d-1\}$ we have:

$$\nu(g_{i_j}) - \nu(g_{i_{j+1}}) = \nu(\xi_{i_j+1}) + \cdots + \nu(\xi_{i_{j+1}})$$

Hence, using $\nu(\xi_{i_{j+1}}) > \nu(\zeta_d) \geq 1$:

$$\nu(\zeta_j) \leq \nu(g_{i_j}) - \nu(g_{i_{j+1}}) \leq (i_{j+1} - i_j)\nu(\zeta_j)$$

By the same argument, for $j \in \{0, \cdots, d-2\}$:

$$\nu(\zeta_{j+1}) \leq \nu(g_{i_{j+1}}) - \nu(g_{i_{j+2}}) \leq (i_{j+2} - i_{j+1})\nu(\zeta_{j+1})$$

Hence,

$$\frac{\nu(g_{i_j}) - \nu(g_{i_{j+1}})}{\nu(g_{i_{j+1}}) - \nu(g_{i_{j+2}})} \geq \frac{\nu(\zeta_j)}{(i_{j+1} - i_j)\nu(\zeta_{j+1})} \geq 2$$

Set $G_j = \nu(g_{i_j})$ for $j = 0, \cdots, d-1$. We know that the G_j are such that $|G_{j+1} - G_j| < \frac{1}{2}|G_j - G_{j-1}|$. Hence

$$\#\{\sum s_j G_j, s_j \in \{0;1\}\} = 2^d$$

Hence:

$$\#\{\nu(\prod_{s\in S} g_s), S \subset \{0, \cdots, D\}\} \geq 2^d$$

and hence

$$\mu(g) = \#\{\sum_{S\subset\{0,\cdots,D\}} \theta_S \prod_{s\in S} g_s, \theta_S \in \{0;1\}\} \geq 2^{2^d}$$

By Lemma 1 in [1] or by Lemma 4 in [2],

$$\mu(g) \leq 2^{(D+1)^{28L^2}}$$

and hence, taking logs:

$$(D+1)^{28L^2} \geq 2^d$$

Taking logs again:

$$28L^2 \geq \frac{d}{\log_2 D + 1}$$

and hence:

$$L \geq \sqrt{\frac{d}{28 \log_2 D + 1}}$$

$\square$

Note: Lemma 1 in [1] is slightly more general than Lemma 4 in [2]. However, using Lemma 4 in [2] it is possible to replace all the appearances of the number 28 in the statement and proof of Lemma 1 above by the number 21.

Proof of Lower Bound 2. We see from its Netwon diagram that the polynomial p has distinct roots $\zeta_1, \cdots \zeta_d$ with:

$$\nu_2(\zeta_i) = 2^{d(d-i+1)} - 2^{d(d-i)} = 2^{d(d-i)}(2^d - 1)$$

So we have $\nu_2(\zeta_d) = 2^d - 1 > 1$, and

$$\nu_2(\zeta_i)/\nu_2(\zeta_{i+1}) = 2^d \tag{3}$$

Assume that there are a, b such that for each d, there is a machine M over $\mathbb{C}$ deciding $p(t) = 0$ in time $T = a(\log d)^b$. Its generic path is defined by a polynomial $g(t)$ of degree $\leq 2^T$.

Let us fix $d > 28(T+1)T^2$. In particular $d \geq T+1$. We are in the conditions of Lemma 1, where $D = 2^T$. From that Lemma, it follows that

$$T \geq \sqrt{\frac{d}{28 \log_2 2^T + 1}} \geq \sqrt{\frac{d}{28(T+1)}}$$

Hence,

$$28T^2(T+1) \geq d$$

contradicting our choice of d. $\square$

Equation (3) holds trivially in the proof of Lower bound 1. The rest of the proof is verbatim the same.

References

[1] Mikel Aldaz, Joos Heintz, Guillermo Matera, José L. Montaña, and Luis M. Pardo. Combinatorial hardness proofs for polynomial evaluation. In Lubos Brim, Jozef Gruska, and Jirí Zlatuska, editors, *Mathematical Foundations of Computer Science 1998, 23rd International Symposium, MFCS'98, Brno, Czech Republic, August 24-28, 1998*, volume 1450 of *Lecture Notes in Computer Science*, pages 167–175, 1998.

[2] Mikel Aldaz-Zaragüeta and José Luis Montaña-Arnaiz. Combinatorial proofs for transcendency of formal power series (extended abstract). Universidad Publica de Navarra, May 1998.

[3] Lenore Blum, Felipe Cucker, Mike Shub, and Steve Smale. *Complexity and Real Computation.* Springer, 1998.

[4] Peter Burgisser, Michael Clausen, and M. Amin Shokrollahi. *Algebraic Complexity Theory.* Grundlehren der mathematischen Wissenchaften 315. Springer, Berlin, 1997.

[5] Serge Lang. *Algebraic Number Theory.* Springer-Verlag, New York, 1986.

[6] Volker Strassen. Polynomials with rational coefficients which are hard to compute. *SIAM Journal on Computing*, 3(2):128–149, 1974.